Docket No. 1152-002U **PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | Customer Number: 29973 |
| Stephen M. HITCHEN. | : | Confirmation Number: 8250 |
| Application No.: 09/992,582 | : | Group Art Unit: 2167 |
| Filed: November 16, 2001 | : | Examiner: Luke S. Wassum |

For: COLLABORATIVE FILE ACCESS MANAGEMENT SYSTEM

**TRANSMITTAL OF APPEAL BRIEF**

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith in Response to the Notification of Non-Compliant Appeal Brief dated January 10, 2007, is Appellant's Appeal Brief in support of the Notice of Appeal with Pre-Appeals Conference Request filed July 5, 2006 and the Notice of Panel Decision from Appeal Review mailed July 26, 2006. A petition for a three-month extension of time under 37 C.F.R. § 1.136 has been previously made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-3839, and please credit any excess fees to such deposit account.

Date: January 16, 2007

Respectfully submitted,

Steven M. Greenberg, Registration No. 44,725
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

Docket No. 1152-002U **PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | Customer Number: 29973 |
| Stephen M. HITCHEN. | : | Confirmation Number: 8250 |
| Application No.: 09/992,582 | : | Group Art Unit: 2167 |
| Filed: November 16, 2001 | : | Examiner: Luke S. Wassum |

For: COLLABORATIVE FILE ACCESS MANAGEMENT SYSTEM

## APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed July 5, 2006, wherein Appellant appeals from the Examiner's rejection of claims 1-20.

## I. REAL PARTY IN INTEREST

This application is assigned to Adhaero Technologies, Inc. by assignment recorded on November 16, 2001, at Reel 012332, Frame 0990.

## II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

## III. STATUS OF CLAIMS

Claims 1-20 are pending in this Application and have been three-times rejected. It is from the multiple rejections of claims 1-20 that this Appeal is taken.

## IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Final Office Action dated April 4, 2006.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 9, 12 and 13 are respectively directed to a collaborative file rights management method, another collaborative file rights management method, a collaborative file rights management system, and a machine readable storage having stored thereon a computer program for managing digital rights in a collaborative file.

In accordance with the Appellants' invention, a file input/output (I/O) request to access a file can be identified (Paragraph [0037], lines 1 through 5). The file I/O request can originate in an authoring application (Paragraph [0034], lines 5 through 9, Paragraph [0037] lines 6 through 9). Thereafter, the file I/O request can be suppressed (Paragraph [0038], lines 1 through 2). Digital rights management data appended to the file can be automatically extracted from the file (Paragraph [0038], lines 2-5) and the file can be provided to the authoring application (Paragraph [0041], lines 1 through 3). Finally, access to the file can be managed in the authoring application based upon the extracted digital rights management data (Paragraph [0041], lines 3 through 5). In this way, an end user loading the file in the authoring application

can remain unaware of the interception and decryption process due to the suppression of the file I/O request and the processing of the appended digital rights management data appended to the file.

## VI. ISSUES TO BE REVIEWED ON APPEAL

1. Claims 1 through 20 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,724,578 to Morinaga et al. (Morinaga) in view of U.S. Patent Application Publication No. 2002/0035697 to McCurdy et al (McCurdy) and further in view of U.S. Patent Application Publication No. 2002/0178271 to Graham et al. (Graham).

## VII. THE ARGUMENT

### THE REJECTION OF CLAIMS 1-20 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON MORINAGA IN VIEW OF MCCURDY AND FURTHER IN VIEW OF GRAHAM.

For convenience of the Honorable Board in addressing the rejections, claims 2-8 stand or fall together with independent claim 1, claims 10-11 stand or fall together with claim 9, and claims 13-20 stand or fall together with independent claim 12.

Graham's interception and modification of a file system request is not the same as the claimed suppression of a file I/O request.

The Examiner's combination of Morinaga with McCurdy and Graham relies exclusively upon the presence of the claimed "suppression" of a file I/O request in paragraphs [0140] and [0141] of the Graham reference. In fact, the Examiner concedes in page 4 of the Final Office Action of April 4, 2006 that neither Morinaga nor McCurdy teach this important claimed feature. The Examiner has cited no other portion of Graham and no other prior art reference for this important teaching. Importantly, the cited portion of Graham wholly lacks any reference to the

**suppression** of file I/O requests as explicitly recited in all of the independent claims. Rather, Graham only teaches the interception and modification of file requests.

In particular, the first sentence of paragraph [0141] of Graham is telling,

> "This filter driver allows the client module 230 to intercept and modify file requests to and from file servers as required."

Accordingly, it will be clear from this statement that file requests are not "suppressed" as required by the language of the Applicants claims 1, 9, 12 and 13, but merely "modified". On page 10 of the Third Response to the Non-Final Office Action dated October 20, 2005, Appellant argued that the Applicants' careful reading of Graham, paragraphs [0140] and [0141], reveal that while a "filter-driver" can be used to "intercept and modify" a file system request, nowhere in paragraphs [0140] and [0141] is it stated or suggested that the "filter-driver" can "suppress" a file system request as required by the language of the Applicants' independent claims. Notwithstanding, the Examiner issued the Final Office Action of April 4, 2006.

Graham's proxy system bears no relation to Graham's filter driver.

Notably, in the Final Office Action of April 4, 2006, the Examiner addressed the Appellants' arguments restated above by claiming that paragraphs [0021] and [0022] teach the crucial quashing/suppressing functionality despite the fact that paragraphs [0140] and [0141] discuss the operation of a filter-driver in a distributed file system on a file I/O request, and paragraphs [0021] and [0022] bear no relationship to the filter-driver discussed in paragraphs [0140] and [0141]. For the convenience of the Honorable Board, the Appellant reproduces the entirety of Graham paragraphs [0021] and [0022] relied upon by the Examiner:

> [0021] The proxy system acts as a file server that mimics the structure and presentation of the content source, for which the proxy system is acting as a

> proxy. When a file is requested by an end-user of client device the proxy system appears (to the end-user) as a file server. To transfer the file from the content source, the proxy system appears to be a network file sharing client (to the content source). These representations occur simultaneously. When an end-user client device requests a file from the network file storage device, the request is received by the proxy system, which selectively provides the requested file as a function of information the proxy system obtains from authentication system and policy system.
>
> [0022] Prior to requesting a file, the user preferably authenticates with authentication system. After authentication, when an end-user requests a file, the proxy system obtains verification of the authentication of the user from the authentication system and in cooperation with the policy system, the proxy system determines if the requesting user has the right to access the file. If access to the file is granted, the proxy system provides the file, in a secure and encrypted manner, with additional information (e.g., usage rights and encryption/decryption keys) to the end-user client device.

Appellants observe that neither the term "filter driver" nor any equivalent thereof appear within the text of paragraphs [0021] and [0022]. Yet, the Examiner has chosen to cure the deficiencies of paragraphs [0021] and [0022] by relying upon the text of paragraphs [0021] and [0022]? Put plainly, there is no disclosure within paragraphs [0021] and [0022] stated above that can be reasonably determined to teach the suppression of a file I/O request as expressly recited in the Appellants' independent claims.

Graham cannot be reasonably combined with Morinaga as Graham teaches the mere modification and forwarding of a file I/O request rather than a suppression of a file I/O request.

Appellants argued in the Third Response to the Non-Final Office Action dated October 20, 2005 that Graham could not reasonably be combined with Morinaga because to do so would destroy the operation of the Appellants' claimed invention. Specifically, the claim language of the Appellants' independent claims expressly require a suppression of an intercepted file I/O request which suppression inherently precludes the forwarding of the file I/O request. Yet,

Graham requires the forwarding of a modified form of an intercepted file I/O request. Accordingly, to combine Graham with Morinaga would defeat the operation of the Appellants' invention rather than arriving at the Appellants' invention. The Examiner to date has not addressed Appellants' arguments in this regard.

Conclusion

Based upon the foregoing, Appellant respectfully submit that the Examiner's rejections under 35 U.S.C. § 103 for obviousness based upon the applied prior art are not viable. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 103.

Date: January 16, 2007

Respectfully submitted,

Steven M. Greenberg
Registration No. 44,725
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

## VIII. CLAIMS APPENDIX

1. A collaborative file rights management method comprising:

identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application;

suppressing said file I/O request;

automatically extracting digital rights management data appended to said file;

providing said file to said authoring application; and,

managing access to said file in said authoring application based upon said extracted digital rights management data.

2. The method of claim 1, further comprising:

decrypting said file.

3. The method of claim 1, wherein said extracting step further comprises:

determining environmental data associated with said file I/O request, said environmental data comprising at least one of a requestor's identity, a requestor's class, a requestor's computing domain, a requestor's location, a password, a time of day, and a date; and,

extracting an access policy appended to said file.

4. The method of claim 3, wherein said providing step comprises:

comparing said access policy to at least a portion of said environmental data;

authenticating said file I/O request based upon said comparison; and,

providing said file to said authoring application only if said file I/O request has been authenticated.

5. The method of claim 1, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

6. The method of claim 1, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to access said file in one of said I/O request packets.

7. The method of claim 1, wherein said management step comprises:

intercepting operating system messages in said authoring application;

detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data; and,

quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

8. The method of claim 7, wherein said authoring application operations comprise operations selected from the group consisting of clipboard operations, printing operations, file saving operations, and file editing operations.

9. A collaborative file rights management method comprising:

identifying a file input/output (I/O) request to save a file, said request originating in an authoring application;

suppressing said request and automatically encrypting said file;

appending an access policy and digital rights management data to said encrypted file; and,

storing said file in fixed storage.

10. The method of claim 9, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

11. The method of claim 9, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to save said file in one of said I/O request packets.

12. A collaborative file rights management system comprising:

a file security management application configured to intercept operating system messages directed to an authoring application; and,

a file security filter driver configured to identify file input/output (I/O) requests received in a kernel-layer file system manager to open an encrypted file in said authoring application;

said file security filter driver quashing said file I/O requests, decrypting said encrypted file and providing said decrypted file to said authoring application;

said file security management application extracting digital rights management data appended to said encrypted file, detecting among intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data, and, quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

13. A machine readable storage having stored thereon a computer program for managing digital rights in a collaborative file, said computer program comprising a routine set of instructions for causing the machine to perform the steps of:

identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application;

suppressing said file I/O request;

automatically extracting digital rights management data appended to said file;

providing said file to said authoring application; and,

managing access to said file in said authoring application based upon said extracted digital rights management data.

14. The machine readable storage of claim 13, further comprising:

decrypting said file.

15. The machine readable storage of claim 13, wherein said extracting step further comprises:

determining environmental data associated with said file I/O request, said environmental data comprising at least one of a requestor's identity, a requestor's class, a requestor's computing domain, a requestor's location, a password, a time of day, and a date; and,

extracting an access policy appended to said file.

16. The machine readable storage of claim 15, wherein said providing step comprises:

comparing said access policy to at least a portion of said environmental data;

authenticating said file I/O request based upon said comparison; and,

providing said file to said authoring application only if said file I/O request has been authenticated.

17. The machine readable storage of claim 13, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

18. The machine readable storage of claim 13, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to access said file in one of said I/O request packets.

19. The machine readable storage of claim 13, wherein said management step comprises:

intercepting operating system messages in said authoring application;

detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data; and,

quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

20. The machine readable storage of claim 19, wherein said authoring application operations comprise operations selected from the group consisting of clipboard operations, printing operations, file saving operations, and file editing operations.

## IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

## X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.